As part of the strict network access policies employed in the State Network, it is important to ensure that malicious traffic is blocked from the network in an expeditious manner. Malicious traffic is defined as data patterns that will cause a threat to confidentiality, integrity or availability of State data. This policy is established in order to provide guidelines for network traffic blocking. (GITA P800-S830 Rev 3.0).

Extreme Performance Degradation, High Security Threat

If traffic in the network causes extreme performance degradation or is deemed a high security threat to an agency, the central network management authority (AZNet), can take immediate reactive measures to block the malicious traffic. If the traffic block is put into operation by blocking the Internet source, AZNet must communicate this block to the agency security contacts as soon as possible. In all instances, AZNet should communicate this block within 2 hours. If the traffic block is put into operation by blocking an agency source, AZNet must immediately communicate this block to the source agency contacts. The affecting agency shall remain anonymous to other agencies in notifications. GITA may be informed of the affecting agency's identity upon request.

No Performance Degradation, Medium/Low Security Threat

If traffic entering the network causes no performance degradation and is deemed a medium or low security risk (i.e. the traffic is reminiscent of a malicious attack), the agency to which the traffic is directed shall be contacted by AZNet as soon as practicable. The agency will have 8 hours to rectify the issue. If, the agency is unable to rectify the issue within this time, AZNet may, at its discretion and for the benefit of the majority of state agencies, block the traffic.

If the traffic block is put into operation by blocking the Internet source, AZNet must communicate this block to the agency security contacts as soon as possible. In all instances, AZNet should communicate this block within 8 hours. If the traffic block is put into operation by blocking an agency source, AZNet must immediately communicate this block to the source agency contacts. The affecting agency shall remain anonymous to other agencies in notifications. GITA may be informed of the affecting agency's identity upon request.

If no specific Agency is the target of traffic that appears to be malicious, AZNet may, at its discretion and for the benefit of the majority of the state agencies, block the traffic. AZNet should communicate this block to the agency security contacts within 8 hours.

Blocking Sources

Where possible, traffic blocks should be limited to host addresses on the Internet source. If, however, the traffic is of the type that will change host addresses within a network, a subnet may be blocked.

Reinstating Sources

If a traffic stream was blocked by this policy, it can be reinstated after remediation and appropriate investigation.